Cybersécurité et l IA :

Qu‘ est-ce que c’est que la cybersécurité ? :

La cybersécurité concerne la protection des systèmes informatiques, des réseaux, des appareils et des données contre des menaces, des attaques ou des accès non autorisés. Elle vise à assurer la confidentialité, l'intégrité et la disponibilité des informations numériques.

Elle englobe plusieurs aspects, parmi lesquels :

* Sécurité des données : Garantir que les données sensibles ne soient pas compromises, qu'elles soient stockées, traitées ou en transit.
* Sécurité des réseaux : Protéger les réseaux informatiques des intrusions, du piratage et des attaques malveillantes.
* Sécurité des applications : Assurer la sûreté des logiciels et des applications utilisées, en les protégeant contre les vulnérabilités et les failles.
* Sécurité des appareils : Protéger les dispositifs tels que les ordinateurs, les smartphones, les objets connectés, etc., contre les atteintes à la sécurité.

La cybersécurité utilise diverses mesures pour protéger ces éléments, y compris des pare-feu, des logiciels antivirus, des protocoles d'authentification, des cryptages, des tests de pénétration et des politiques de sécurité strictes. Elle nécessite également une surveillance constante pour détecter et répondre aux menaces émergentes.

En raison de l'évolution rapide des technologies et des menaces, la cybersécurité est un domaine en constante évolution, nécessitant une adaptation continue pour faire face aux nouvelles stratégies d'attaques et aux failles de sécurité potentielles.

Qu est ce que c’est l’ia ? :

L'intelligence artificielle (IA) est un domaine de l'informatique qui se concentre sur la création de systèmes et de machines capables de réaliser des tâches qui nécessitent normalement l'intelligence humaine. Son objectif est de simuler certains aspects du comportement humain afin d'améliorer l'efficacité, l'automatisation et la précision des processus dans divers domaines.

Elle englobe plusieurs aspects, parmi lesquels :

* Apprentissage automatique (Machine Learning) : La capacité des machines à apprendre à partir de données et à améliorer leurs performances sans être explicitement programmées.
* Traitement du langage naturel (NLP) : La capacité des machines à comprendre et à interagir avec le langage humain, y compris la reconnaissance vocale, la compréhension de texte et la génération de texte.
* Vision par ordinateur : La capacité des machines à interpréter et à comprendre des images et des vidéos, souvent utilisée dans la reconnaissance faciale, la détection d'objets et la classification d'images.
* Robotique : L'utilisation de l'IA pour concevoir des robots capables d'effectuer des tâches physiques et cognitives, souvent dans des environnements complexes et changeants.

L'IA utilise diverses techniques et algorithmes, notamment les réseaux de neurones, les arbres de décision, les algorithmes génétiques, etc. Elle nécessite également des ensembles de données volumineux pour l'entraînement et des ressources informatiques puissantes pour le traitement.

En raison de son évolution constante et de son potentiel à transformer de nombreux secteurs, l'IA est au cœur de nombreuses innovations et discussions sur son impact sur la société, l'éthique et l'avenir du travail.

Méthode de recherche :

Feedly

dernières évolutions :

En termes de changements dans le domaine de la cybersécurité causé par l ia nous pouvons cité :

* Layer x security qui utilise l ia dans son logiciel de protection des navigateurs, cette entreprise à réussi à levé 26 millions de fonds
* Des pirates iraniens qui ont lancé des attaques qui ont été décrites comme très ciblées et bien planifiées. Les hackers ont utilisé des tactiques telles que l'envoi de courriels de phishing soigneusement conçus pour inciter les victimes à divulguer leurs informations d'identification. Ils ont également exploité les réseaux sociaux pour obtenir des informations personnelles sur leurs cibles, facilitant ainsi la personnalisation des attaques.
* Risques liés à l’IA générative S'appuyant sur le groupe de travail sur l'IA générative du NIST, le « AI RMF Generative AI Profile » (NIST AI 600-1) répertorie 13 risques liés à l'IA générative, notamment le codage de logiciels malveillants, l'automatisation des cyberattaques, la propagation de la désinformation, l'ingénierie sociale et les hallucinations de l'IA (« confabulation »). Les systèmes d’IA de première génération d’aujourd’hui sont capables de synthétiser de manière malveillante des images, du son et des vidéos suffisamment bien pour qu’il soit impossible de les distinguer du contenu authentique.
* L'article souligne que la ActiveAI ne se contente pas de détecter les menaces connues, mais qu'elle identifie également de nouveaux modèles d'attaque et adapte ses réponses en conséquence. Cette approche proactive vise à renforcer la résilience globale des organisations face aux menaces cybernétiques en constante évolution, leur permettant de rester en avance sur ces menaces.

sources :

<https://www.csoonline.com/article/2097761/layerx-security-raises-26m-for-its-browser-security-platform-enabling-employees-to-work-securely-from-any-browser-anywhere.html>

<https://www.csoonline.com/article/2097509/iranian-hackers-harvest-credentials-through-advanced-social-engineering-campaigns.html>

<https://www.csoonline.com/article/2097119/nist-publishes-new-guides-on-ai-risk-for-developers-and-cisos.html>

<https://fr.darktrace.com/blog/moving-beyond-xdr-to-achieve-true-cyber-resilience-with-darktrace-activeai-security-platform>